

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**BEST AVAILABLE COPY**

Appl. No. 09/603,356

**REMARKS/ARGUMENTS**

On page 2 of the Office Action, the Examiner notes in the "Response to Arguments" section that failure to traverse Official Notice statements made in previous Office Actions serves as evidence of Applicant's admission that asserted features are in fact well known in the art. This appears to be a default position taken by the Patent Office in accordance with Subsection 2144.03(C) of the MPEP. However, all of the submissions made in response to preceding Office Actions related to establishing a date of invention prior to the date of a previously cited reference, by way of a 37 CFR 1.131 D declaration. In view of the fact that one of the references which had been relied upon for all claim rejections was rendered uncitable, it is respectfully submitted that there was no requirement to provide detailed arguments in respect of the other issues raised in the claim rejections. The claim rejections were effectively rendered moot by a finding that the previously cited M2 reference was not citable. Indeed, one of the primary advantages of submitting a declaration under 37 CFR 1.131 is that detailed arguments need not be placed on the official record. Accordingly, it is submitted that the responses to previous Office Actions should in no way be construed as including or implying an admission that the asserted features are known in the art. Applicant hereby further makes a clear statement on the record that Applicant does not admit that the asserted features are in fact well known in the art.

Turning now to the claim rejections under 35 USC 103(a), claims 1-22, 24-26, and 31-35 were rejected as being unpatentable over Parker ("Single Sign-On Systems – The Technologies and the Products", 1995) in view of PR Newswire ("Microsoft Passport Offers Streamlined Purchasing Across Leading Web Sites", October 11, 1999, hereinafter referred to as "PR"). However, as discussed in further detail below, each of these claims recites features which have not been disclosed or suggested in, and thus would not be obvious in view of the cited references, alone or in combination.

In rejecting claims 1, 24, and 26, page 3 of the Office Action asserts that Parker discloses the method recited in claim 1, with the exception of the claimed feature that two network devices between which access control information is conveyed are on different domains.

Appl. No. 09/603,356

On page 152, Parker describes an authentication and access scheme whereby a user authenticates to a remote authentication server and receives in return a data token or certificate referred to as an authentication ticket, which can subsequently be used to prove the user's authenticity. When the user selects a target application server to access, this authentication ticket is used to obtain from a remote security server, which along with the authentication server is part of a single sign-on product, an access ticket which is suitable for use in accessing the target application server. From page 3 of the Office Action, it is apparent that the Examiner is interpreting Parker's remote security server as being one network device, the authentication ticket as being access control information, the access ticket as being a response message, and the target application server as being another network device.

Although Parker characterizes the access ticket as being suitable for use in accessing a target application server, no information is provided as to the content of an access ticket. Parker is similarly silent on the content of the authentication ticket. Therefore, the particular information which is transmitted between any of the servers and a user workstation in Parker is not apparent from the reference.

In particular, there is no disclosure or suggestion in Parker that the access ticket is in any way adapted to cause a message to be sent to the target application server. Therefore, Parker fails to disclose or suggest at least the claimed feature "the response message being adapted to cause the end user device to send a second message to the another network device containing at least part of the access control information", as recited in claim 1. Parker merely refers to a target application server receiving the access ticket, without providing any indication whatsoever as to a transfer mechanism for sending the access ticket to the target application server.

At the bottom of page 3 of the Office Action, it is acknowledged that Parker also does not disclose network devices on different domains. The subsequent statement that Parker indicates that the two servers are part of the single sign-on product, which is relied upon in concluding that allowing single sign-on to network devices from different domains in a single sign-on system is well known, appears to apply a different interpretation of Parker than the above

Appl. No. 09/603,356

interpretation used in asserting that other features of claim 1 have been disclosed in the reference.

As described above, it is clear from the rejection of claim 1 that the remote security server and the target application server are interpreted by the Examiner as being analogous to one network device and another network device, respectively. However, the two servers which Parker discloses as being part of a single sign-on product are the authentication server and the remote security server. These servers do not operate in a manner which is consistent with the method as recited in claim 1, as Parker does not disclose protected resources associated with the authentication server and the remote security server. It is thus submitted that this interpretation of Parker differs significantly from the subject matter recited in claim 1. It is further submitted that a combination of two different interpretations of the same reference is not a proper basis for claim rejections.

On page 4 of the Office Action, it is asserted that PR discloses a multi-domain single sign-on system that allows participation by Internet domains owned by different companies or business partners. This reference, however, provides no technical detail on how to convey access control information from one network device to another network device on a different domain through an end user device. In the absence of any such technical details, it is submitted that it would not be obvious from PR that the system disclosed therein could be used to convey access control information between network devices on different domains.

More specifically, the "PR" as cited by the examiner provides no technical detail on how to convey access control information from one network device to another network device on a different domain through an end user device. In the absence of any technical details in the "PR" which may be useful to an ordinary person skilled in the art, it is not obvious from the "PR" that it is possible convey access control information from one network device to another network device on a different domain through an end user device. Although not addressed by the "PR", the HTTP protocol and HTTP cookies are well known mechanisms for maintaining single sign-on within a single domain and should be understood by an ordinary person skilled in the art.

Appl. No. 09/603,356

However, the same person would also be familiar with the limitations of HTTP cookies and available HTTP browser technologies to know that cookies alone cannot be relied upon to propagate authentication and a.c.i. between two different domains. The reason is that the cookie specification and browser explicitly forbid the forwarding of a cookie created in one domain to a second unrelated domain. Although aspects of our invention may use the HTTP protocol and cookies to maintain single sign-on within a single domain amongst the different domains, some embodiments of the invention solves the practical problem that would have faced an ordinary person skilled in the art at the time, of propagating access control information from one domain to a completely unrelated domain.

The "PR" paragraph cited by the examiner, "Passport allows consumers to use a single sign-in name and electronic wallet at participating sites, reducing the amount of information they need to remember and retype", implies that a single sign-in name is required and that a central authentication server is required. The subject claims do not specify that a single sign-in name be required between domains. It is not obvious from the "PR" that a single sign-in name can be avoided. The requirement for a single sign-in name, provided by a third-party or central authentication server, may be highly undesirable from the view of a domain owner. The subject claims do not require a central authentication server to achieve single sign-on between different domains. Each domain may have its own authentication server. As already stated, a central authentication server has several disadvantages.

In respect of claim 2, page 4 of the Office Action states that Parker further discloses that a response message contains access control information in the form of an access ticket and a network device identifier for another network device, that receipt of the access ticket instructs the user device to access the another network device, and that the second message contains at least part of the access control information, in the form of the access ticket. However, as discussed above, contents of the authentication ticket and the access ticket have not been disclosed in Parker. There is also no disclosure in Parker that receipt of the access ticket instructs the user device to access the another network device. At least these features distinguish claim 2 over Parker.

Appl. No. 09/603,356

At the bottom of page 4, the Examiner takes official notice that including information in either the header or content portion of a data packet is well known in the art. It is respectfully submitted that embedding a network device identifier for the another network device in the content portion of a response message which is sent from the one network device to the end user device would not be obvious. In this case, the embedded network identifier relates to a different network device than the network device from which the response message is sent to the end user device. This is not known in the art.

With regard to claim 3, it is stated on page 5 of the Office Action that Parker further discloses extracting access control information from a packet for use in a response message, and in particular that the access ticket is extracted from a response and placed in a second message for delivery to a target application server. Parker, however, does not disclose or suggest any such functions. There is simply no mention of information extraction or any analogous operation in Parker. The Applicant further asserts that including access control information in the header portion of a message, as recited in claim 3 is not commonly known, and would not be apparent to a person skilled in the art from either of the cited references.

Claim 4 recites a feature of extracting access control information from a first message, which has not been disclosed in Parker as discussed above.

Claim 5 depends from claim 2 and thus distinguishes over Parker for at least the reasons discussed above with reference to claim 2.

Each of claims 6, 12, and 16 recites a control function in relation to the second message transmitted from the end user device to the another network device. According to claim 6, an option to send the second message or not is presented to the end user device. In claim 12, an option to change and/or delete user-specific information before sending the second message is presented to the end user device. Claim 16 recites a similar feature of requiring user acceptance before including user-specific information in the second message.

On page 6 of the Office Action, the Examiner takes official notice that changing user profile information in a network access system is well known in the art. Applicant respectfully

Appl. No. 09/603,356

submits that controlling the second message or the content thereof in the manner recited in these claims, in the context of a method of conveying access control information between network devices in different domains, is not well known. In this particular context, conventional wisdom would teach away from allowing intervention on the part of the end user. It is therefore not obvious from Parker and PR that optional end user intervention is a desirable feature as part of a single sign-on process.

Further, while changing user profile information and network access system may be well known within the context of individual domains, this is not the case when extended to multiple domains. On the contrary, a person skilled in the art would likely be aware of the limitation that HTTP cookies can only be used for maintaining single sign-on within a single domain. Given this well known limitation of HTTP cookies, which are often used for maintaining single sign-on within a single domain, it would not be obvious that changing user profile information between domains can be part of a single sign-on process between different domains.

The remarks made in the paragraph bridging pages 6 and 7 of the Office Action with reference to claim 7 are not entirely understood. Claim 7 recites formatting of the content portion of a response message as a custom content type. With reference to claim 2, from which claim 7 depends, the content portion of the response message contains access control information and a network device identifier, which according to claim 7 are formatted as a custom content type. At line 2 of page 7 of the Office Action, reference is made to gaining access to personalized, customized information. With respect, Applicant points out that the custom content type recited in claim 7 relates to access control information and a network identifier, whereas the comment in the Office Action appears to refer to customized information which may be subsequently accessed.

Each of claims 8-10 depends from either claim 1 or claim 2 and thus distinguishes over the cited references for at least the reasons discussed above. Claims 9 and 10 further distinguish over the cited references, as well as conventional HTTP messages and cookies, in that the use of such messages and cookies in a multiple-domain system in the manner recited in the claims is not known in the art.

Appl. No. 09/603,356

In regard to claims 11 and 14, the cited references do not disclose or suggest the claimed feature of a response message containing user-specific information together with instructions to include at least part of the user-specific information in the second message. Although PR mentions "extensive customization" and an electronic wallet that stores billing and shipping information, there is no mention of an instruction to control the particular information transferred within the Passport product described therein.

A reference to accessing personalized information on line 2 of page 8 of the Office Action also appears to indicate an incorrect interpretation of these claims, as discussed above with reference to claim 7.

In rejecting claim 13, it is asserted that Parker discloses an initial network device, in the form of an authentication server, which receives an initial access request from an end user device to access a protected resource on the initial network device. However, Parker has not disclosed any protected resource on the remote authentication server. The authentication server authenticates a user, but does not itself support any protected resources. Thus, the feature recited in clause a) of claim 13 has not been disclosed or suggested in Parker.

Page 8 of the Office Action also states that Parker discloses the claimed feature of the initial network device causing the end user device to send the first message. No such operation has been disclosed or suggested in Parker.

Even if Parker's remote authentication server and remote security server were merged into a single device, as suggested in the Office Action, the single device would not operate in accordance with the method recited in claim 13. At least the above features would not be found in the merged device.

Claims 15 and 17 depend from claim 1 through claim 14 and claim 13, and thus distinguish over the cited references for the reasons discussed above with reference to these claims.

Claim 18 includes features similar to those recited in claims 1, 2, and 4 and thus similarly distinguishes over the cited references.



Appl. No. 09/603,356

In regard to claim 19, it is respectfully submitted that Parker does not disclose or suggest that the another network device is specified in a message. Although Parker mentions that a user selects a target application server to access, details of any transfer mechanisms used between the elements of the Parker system have not been disclosed in the reference. Similarly, the feature that the another network device is specified by the network device, as recited in claim 20, is also absent from Parker.

Independent claim 21 recites features similar to those of claims 18 and 13 and thus distinguishes over the cited references for similar reasons. The additional feature of a redirect message instructing a redirection and specifying access control information in a header of the redirect message further distinguishes claim 21 over the cited references.

Claim 22 depends from claim 21 and recites the further feature of responding to an initial access request message with a redirect message if an authentication process determines that access should be granted. No such features have been disclosed or suggested in Parker.

Claim 25 depends from claim 18 and thus distinguishes over the cited references for at least the reasons discussed above.

Claims 31-34 include similar features to those recited in claim 21, as indicated by the Examiner on page 11 of the Office Action, and thus similarly distinguish over the cited references.

Claim 35 distinguishes over the cited references for at least the reasons discussed above with reference to claims 1, 2, 11, and 12, as similar features have been recited in claim 35.

It is thus respectfully submitted that claims 1-22, 24-26, and 31-35 patentably distinguish over the cited references for at least the above reasons, and that the obviousness rejections should be reconsidered and withdrawn.

The Examiner is thanked for the allowance of claims 23 and 27-30. For the reasons discussed in detail above, it is believed that rejected claims 1-22, 24-26, and 31-35 are also allowable.


Appl. No. 09/603,356

In view of the forgoing, early favorable consideration of this application is earnestly solicited.

Respectfully submitted,

RAY C.H. CHENG ET AL.

By

  
Allen Brett

Reg. No. 40,476

Tel.: (613) 232 2486 Ext. 323

Date: August 16, 2004  
RAB/DMW/map  
Ottawa, Ontario, Canada